AD-A243 770

(2)

NAVAL POSTGRADUATE SCHOOL

Monterey, California

DTIC
ELECTE
DEC 3 1 1991
S D
D

THESIS

A COMPARISON OF DATA INTEGRITY MODELS

by

Thomas R. Ivan

March, 1991

Thesis Advisor: Moshe Zviran

Approved for public release; distribution is unlimited

91-19153

91 1227 021

Unclassified

SECURITY CLASSIFICATION OF THIS PAGE

REPORT DOCUMENTATION PAGE

1a. REPORT SECURITY CLASSIFICATION
Unclassified

1b. RESTRICTIVE MARKINGS

2a. SECURITY CLASSIFICATION AUTHORITY

2b. DECLASSIFICATION/DOWNGRADING SCHEDULE

3. DISTRIBUTION/AVAILABILITY OF REPORT
Approved for public release; distribution is unlimited.

4. PERFORMING ORGANIZATION REPORT NUMBER(S)

5. MONITORING ORGANIZATION REPORT NUMBER(S)

6a. NAME OF PERFORMING ORGANIZATION
Naval Postgraduate School

6b. OFFICE SYMBOL *(If applicable)*
55

7a. NAME OF MONITORING ORGANIZATION
Naval Postgraduate School

6c. ADDRESS *(City, State, and ZIP Code)*
Monterey, CA 93943-5000

7b. ADDRESS *(City, State, and ZIP Code)*
Monterey, CA 93943-5000

8a. NAME OF FUNDING/SPONSORING ORGANIZATION

8b. OFFICE SYMBOL *(If applicable)*

9. PROCUREMENT INSTRUMENT IDENTIFICATION NUMBER

8c. ADDRESS *(City, State, and ZIP Code)*

10. SOURCE OF FUNDING NUMBERS

Program Element No	Project No	Task No	Work Unit Accession Number

11. TITLE *(Include Security Classification)*
A Comparison of Data Integrity Models

12. PERSONAL AUTHOR(S) Thomas R. Ivan

13a. TYPE OF REPORT
Master's Thesis

13b. TIME COVERED
From To

14. DATE OF REPORT *(year, month, day)*
March 1991

15. PAGE COUNT
88

16. SUPPLEMENTARY NOTATION
The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.

17. COSATI CODES

FIELD	GROUP	SUBGROUP

18. SUBJECT TERMS *(continue on reverse if necessary and identify by block number)*
Data Integrity, Data Integrity Models, Biba Model, Goguen and Meseguer Model, Clark/Wilson Model

19. ABSTRACT *(continue on reverse if necessary and identify by block number)*

Data integrity in computer-based information systems is a concern because of the damage that can be done by unauthorized manipulation or modification of data. While a standard exists for data security, there currently is not an acceptable standard for integrity. There is a need for incorporation of a data integrity policy into the standard concerning data security in order to produce a complete protection policy. There are several existing models which address data integrity. The Biba, Goguen and Meseguer, and Clark/Wilson data integrity models each offer a definition of data integrity and introduce their own mechanisms for preserving integrity. Acceptance of one of these models as a standard for data integrity will create a complete protection policy which addresses both security and integrity.

20. DISTRIBUTION/AVAILABILITY OF ABSTRACT
☒ UNCLASSIFIED/UNLIMITED □ SAME AS REPORT □ DTIC USERS

21. ABSTRACT SECURITY CLASSIFICATION
Unclassified

22a. NAME OF RESPONSIBLE INDIVIDUAL
Prof Moshe Zviran

22b. TELEPHONE *(Include Area code)*
(408)646-2498

22c. OFFICE SYMBOL
54Zv

83 APR edition may be used until exhausted
All other editions are obsolete

SECURITY CLASSIFICATION OF THIS PAGE
Unclassified

Approved for public release, distribution is unlimited.

Comparison of Data Integrity Models

by

Thomas R. Ivan
Captain, United States Marine Corps
B.S., United States Naval Academy, 1984

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN INFORMATION SYSTEMS

from the

NAVAL POSTGRADUATE SCHOOL
March 1991

Author: ______________________
Thomas R. Ivan

Approved by: ______________________
Moshe Zviran, Thesis Advisor

____
LTC Rayford B. Vaughn, USA, Second Reader

____
David R. Whipple, Chairman,
Department of Administrative Sciences

ABSTRACT

Data integrity in computer-based information systems is a concern because of the damage that can be done by unauthorized manipulation or modification of data. While a standard exists for data security, there currently is not an acceptable standard for integritv. There is a need for incorporation of a data integrity policy into the standard concerning data security in order to produce a complete protection policy. There are several existing models which address data integrity. The Biba, Goguen and Meseguer, and Clark\Wilson data integrity models each offer a definition of data integrity and introduce their own mechanisms for preserving integrity. Acceptance of one of these models as a standard for data integrity will create a complete protection policy which addresses both security and integrity.

DTIC COPY INSPECTED

Accesion For

NTIS CRA&I ☑
DTIC TAB □
Unannounced □
Justification ....

By ....
Distribution /

Availability Codes

Dist | Avail and / or Special
A-1

TABLE OF CONTENTS

I. INTRODUCTION

A. THE INTEGRITY PROBLEM

Data integrity in computer-based information systems is a concern because of damages that can be done by unauthorized manipulation or modification of data. Such manipulation or modification can happen either maliciously or accidentally when users access data and perform alterations. While the historical emphasis in both military and commercial environments has been placed on controlling access to classified data, this control is effective in limiting disclosure, and preventing unauthorized disclosure. However, it is not a sufficient countermeasure to prevent manipulation or modification by users of classified data. The emphasis on controlling access to data has served to mask the issue of data integrity. The data may be accessible only to authorized individuals, but a mechanism to prevent users, both authorized and unauthorized, from manipulating or modifying that data is also needed. Manipulation or modification compromises the data and, in many situations, can be more harmful than disclosure to an unauthorized user. This raises the thought that there needs to be a way to prevent, or at least detect, unauthorized manipulation as well as unauthorized disclosure. The Department of Defense (DoD) Trusted Computer System

Evaluation Criteria (TCSEC) document [Ref. 1], which establishes policies and principles for data security, does not address data integrity. The scope of this thesis is to define the term data integrity, discuss and analyze three existing data integrity models, compare them, and assess their relevance to DoD applications.

B. INTEGRITY DEFINED

There are many definitions for integrity that are used concerning protection of data. Each model presented in this thesis uses a definition of integrity that has been established by its author(s). For example, Biba [Ref.2:p. 13] defines data integrity in terms of the performance of subsystems that constitute a computer system. In this context, Biba considers a subsystem to be a "subset of a system's subjects and objects isolated on the basis of function." Clark and Wilson [Ref. 3] define data integrity as data that is free from unauthorized manipulation. While there are similarities in the definitions and their applications, they are different. The difficulty with the lack of an accepted definition is that each author establishes guidelines for what his model needs to do based on how the author himself defines integrity. This makes the creation of a standard extremely difficult.

Another definition of data integrity appears in [Ref. 4:p. 335]. This definition covers six areas:

a. How correct the information is thought to be

b. Confidence level that the information is from the original source

c. Correctness of the functioning of the process using the information

d. Level of correspondence of the process function to the designed intent

e. How correct the information in an object is initially

f. Confidence that the information in an object is unaltered

This definition appears to be comprehensive since it covers all the areas that logically fall under the heading of integrity. For instance, the ability to prevent unauthorized manipulation of data is helpful only if the data is correct when received. If it is known with a high degree of confidence that the data is from the original document and it is correct, then integrity must be maintained. If the data is altered in any way before it is received, and unfortunately this may not be detectable, then maintaining integrity will do nothing more than keep the data in its current incorrect, altered state. The definition given above will serve as a reference framework to examine the definitions of integrity on which the three models are based.

C. INTEGRITY CONCERNS

A first concern associated witn data integrity is the lack of work done in this area as compared with the area of data security. The TCSEC [Ref. 1], commonly called the Orange Book, fully describes a set of criteria for protection of classified information. This publication, however, does not address data integrity in the detail it does for security, thereby failing to establish guidelines for integrity policies. The recent attention placed on data integrity is due to a sAifting of emphasis to the area of control of sensitive but unclassified information, which has data integrity as one of its main concerns. The main direction of effort within DoD has been the control of classified data. Security classifications are assigned that allow only those individuals with a proper security clearance access to classified, or controlled, data. Historically, controlling access to data has been considered the main function of any security system within DoD.

The lack of an accepted definition for integrity prevents the development and eventual acceptance of a standard data integrity model, which is a second problem area. As mentioned earlier, the Orange Book has established guidelines concerning data security and access control. A similar publication about data integrity would create a standard definition and possibly a standard model to be used for DoD applications. The models presented in this thesis are compared and recommendations are made based on what was learned through independent research, not on an established guideline. This can lead to problems because, just as in the case of defining integrity, many different opinions can be stated and defended with no correct answer as to which model best serves to maintain data integrity.

D. APPLICABILITY

The idea of data integrity has been presented as a legitimate problem that needs to be addressed. Given this, the question now is who needs to be concerned with data integrity. The answer to this question is that any business or organization where there is more than one person with access to data needs to be aware of data integrity. Organizations that have a well- established security policy cannot consider their policy complete unless it addresses integrity as well as security and control. This is because the manipulation of data is just as harmful as the unauthorized disclosure of that data. The large number of individuals accessing data within DoD dictates a need for a standard integrity policy. The purpose of this thesis is to determine which of the three models presented is most appropriate for application to DoD environments.

This thesis presents the three data integrity models and discusses the advantages and disadvantages of each. Then, a framework for comparison will be developed. This framework is used to compare the models and to try to select one specific model that best matches DoD needs. The models under investigation are:

1. The Biba Model. [Ref.2]
2. The Goguen and Meseguer Model. [Ref. 5]
3. The Clark and Wilson Model. [Ref. 3]

II. BIBA INTEGRITY MODEL

A. INTRODUCTION

The Biba Model [Ref. 2] is the result of work done for the U.S. Air Force by the MITRE Corporation in 1977. A report prepared by K.J. Biba presented the results of this research project and became known as the Biba Model for system integrity.

Biba develops his integrity model using the approach that integrity is the dual of secrecy. He presents several different policies for protection of integrity and tailors each policy for implementation in a Multics environment. This model is often mentioned as the dual of the Bell-LaPadula Model, which is the quasi-standard for [Ref. 1].

B. DEFINITION OF INTEGRITY

The definition of integrity developed in the Biba model addresses a computer system rather than the system data. Biba defines system integrity as "a guarantee that a subsystem will perform as it was intended to perform by its creator." This definition covers the subsystems which combine to make up the overall system. Biba uses the term "subsystem" to represent any subset of a system's subjects and objects that has been isolated based on functionality. An assumption is made by the author that an external verification has been performed on any specific subsystem and that it is functioning properly. This means that each subsystem, and therefore the entire system, is in a state worthy of protection.

Biba points out that possession of the property of integrity will not guarantee the absolute behavior of a system or subsystem. He states that a system will behave as it was designed if it has integrity. The system will perform up to an established standard. The quality of the standard is unimportant. As far as integrity is concerned it does not matter what the system does as long as it behaves according to its design.

As mentioned above, Biba's definition of integrity addresses system components instead of specific data. The process that each subsystem executes is the target of Biba's model. The goal of this model is to prevent unauthorized manipulation of subsystems thereby safeguarding their ability to behave in a manner that is within their design specifications.

Biba's focus on system and subsystem behavior allows him to identify specific threats to system integrity. Preservation of each process in its initial state (possessing the property of integrity) will ensure that the functionality of the entire system is within design constraints.

C. DESCRIPTION

A basic premise of the Biba model is the concept of "no read-up, no write-down" between different integrity levels. These actions can violate the integrity of data at specific integrity levels by allowing users, subjects, or processes to access information for which they are not cleared. A user, subject, or process which is authorized to access low-integrity level data should not be able to access, or read, high-level data. Also, low-level data should not be allowed to enter into any process which uses high-level data. Low-level data has a greater possibility for unauthorized manipulation and therefore it can be contaminated. High-level data can likewise be contaminated if low-level data is allowed to enter into a process using the high-level data. This restriction prevents a low-level authorized user from accessing high-level data and possibly destroying the integrity of that high-level data.

The "no write-down" constraint prevents high level data from being written to low-level object , This eliminates the possibility of destroying the integrity of high-level data by allowing access to unauthorized subjects. High-level data cannot be written down to processes which use low-level data. Data used in high-level processes must remain at the high-level classification and is authorized for use only by other high -level processes.

Biba implements his "no read-up, no write-down" restriction through the application of two classes of integrity policies: mandatory controls and discretionary controls. These two classes constitute the framework of the Biba model. The policies within each class are discussed in this section. The mandatory policies are presented first followed by the discretionary policies.

A mandatory policy is one that reflects the idea that "certain functions, central to the enforcement of the policy, are designed as a fundamental characteristic of the system" [Ref. 3:p. 187]. These are requirements that cannot be bypassed, avoided, or altered by users. Each policy under the category of mandatory must fulfill two requirements. The first is that the policy must identify the objects that require protection. The second is that the policy must determine when requests to access data are permissible. This is the access control for the system. Each of the three policies presented by Biba meets these criteria. The policies use different constraints to limit data access while identifying protected objects for the system.

Throughout his model, Biba refers to subjects and objects when discussing the integrity constraints within each policy. Biba defines a subject as the system element which performs data accesses. He defines an object as those system elements which are accessed. These definitions apply for each occurrence of a subject or an object in the different integrity policies, both mandatory and discretionary.

Biba uses classification levels for integrity that are applicable to either military or commercial environments. The classifications of Top Secret, Secret, and Confidential [Ref. 1] can be used but are not the only possibilities. Labels such as High, Medium, and Low can be assigned to objects within the policies discussed by Biba.

1. Mandatory Integrity Policy

a. *Low-Water Mark Policy*

The Low-Water Mark Policy is based on the premise that the integrity level of the subject is dynamic and will change based on its previous behavior. The integrity level of the subject will be determined by the integrity level of the most recently accessed object. The integrity level of the objects in the system will not change. The data in the objects remains at a constant level with the collection of subjects permissible to access those objects constantly changing.

In this policy it is possible for a subject to downgrade its own integrity level to the lowest level in the system, hence the name low-water mark. Access to the lowest level objects will decrease the integrity level of the subject to the lowest level. This is the biggest drawback of the policy. The subject that reduces its own integrity level to the low-water mark can only be restored to a higher integrity level by reinitializing the entire system. This is obviously not an event that should occur frequently. The policy allows for altering integrity levels downward but it does not allow subjects to increase their integrity level.

The Low-Water Mark Policy is depicted in Figure 1. In this figure, the subject (S1) possesses a High integrity level before it accesses object O2. This means that S1 is authorized to access objects that are labelled High (such as O1). When S1 expands its domain and attempts to access O2 the following occurs. First, the access is granted and second, S1 is assigned an integrity level of Medium. This results from the fact that the level of O2 is Medium. S1 has downgraded its own integrity level from High to Medium by requesting and being granted access to O2. O1 is now out of S1's domain and can not be accessed by S1. Any subsequent actions by S1 to access objects with lower integrity levels than O2 (i.e. Low) will result in the integrity level of S1 being further reduced. The goal of this policy is to prevent the indirect sabotage of object integrity by subjects.

b. Ring Policy

The Ring Policy is designed to address attempts by subjects to directly modify objects. This policy fixes the integrity levels of both subjects and objects and holds these levels constant. This policy increases the flexibility of the system by allowing observation of objects at any level. Subjects are allowed to observe any object, even those objects which possess a higher integrity level than the subject. The trade-off for increased flexibility is decreased integrity assurance. Observation of all objects by all subjects increases the possibility of contamination of data contained in high-level objects.

The Ring Policy allows universal observation of objects but puts constraints on the ability to modify objects. The only modifications allowed are those attempted by a subject on an object that has a less than or equal to integrity level. This prevents low-level subjects from modifying higher-level objects. The subjects can observe the higher-level objects but can not modify these objects. This policy is demonstrated by the example in Figure 2.

In Figure 2, a subject S1 has the ability to observe an object at any integrity level. S1 can observe objects O1, O2, and O3 but can only modify those objects which are at an equal to or less than integrity level, specifically O2 and O3. This shows that S1 can modify O2 and O3 but does not have the ability to modify O1. All three objects are within the domain of S1 because of S1's ability to observe the objects. Restrictions apply only to modification of objects thereby maintaining the integrity of the objects.

c. *Strict Integrity Policy*

The Strict Integrity Policy performs the same functions as the Low-Water Mark Policy but it does so in a different manner. The Strict Integrity Policy does not change the integrity level of a subject. The Low-Water Mark Policy prevents contamination of high-integrity objects by changing the integrity level of subjects to the integrity level of the object most recently accessed. The Strict Integrity Policy forbids access by lower level subjects to a higher level object. The subject's integrity level remains constant. Access requests to levels which exceed the subject's level are denied. The integrity levels of both subjects and objects are static and are externally defined. The system itself can not change integrity levels. Figure 3 illustrates this policy.

Subject S1 possesses an integrity level of Medium. This gives S1 the ability to observe and modify objects at the Medium and Low levels. In this case, S1 can observe and modify objects O2 and O3. S1 does not have the capability of observing objects at the High integrity level. S1's level will not change even though it may observe and modify lower level objects. This constant subject integrity level is the difference between the Strict Integrity Policy and the Low-Water Policy.

The Strict Integrity Policy can be summarized by saying that a subject may read an object if that object's integrity level is greater than the subject. Additionally, a subject may write to an object if that object's integrity level is less than or equal to the subject's level [Ref.6:p. 204].

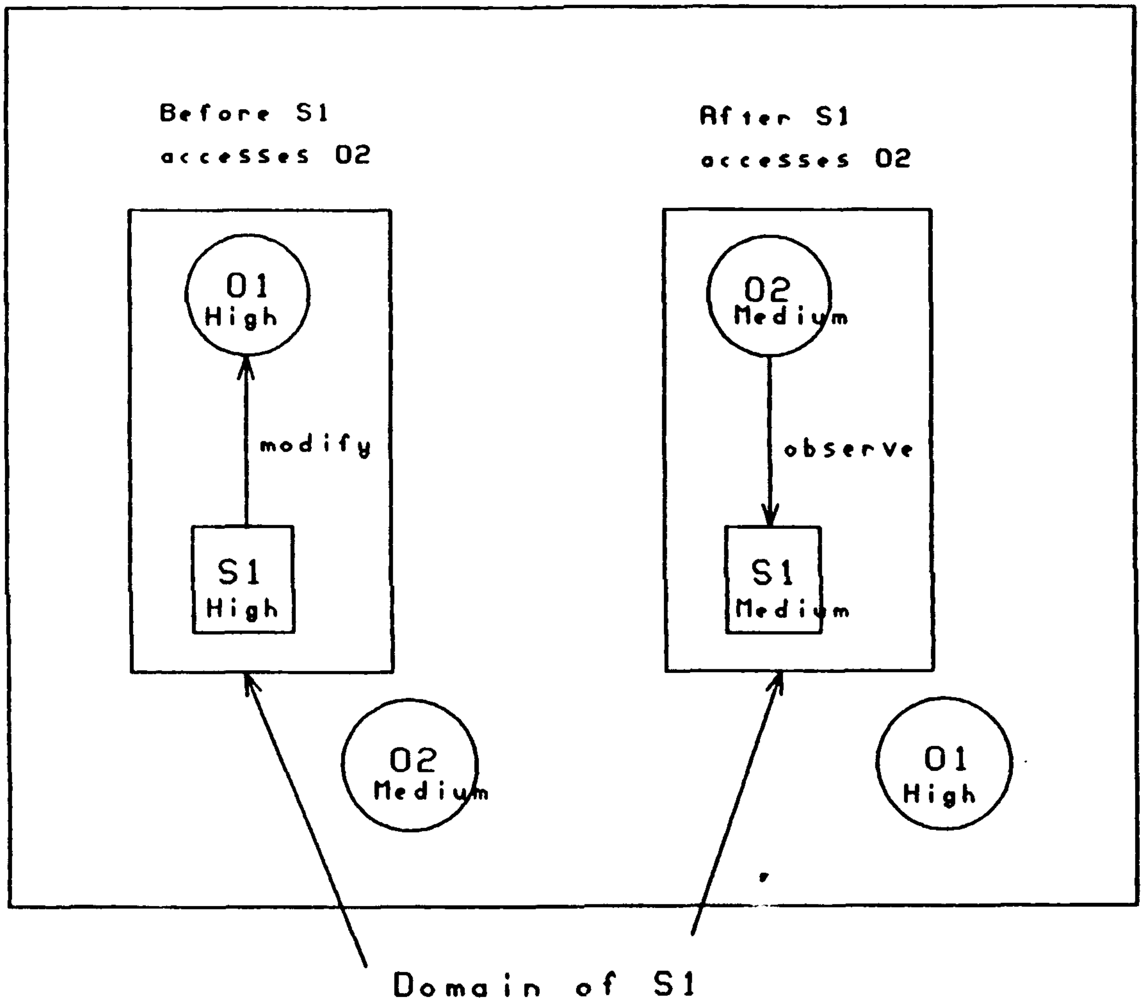


Figure 1 Low-Water Mark policy

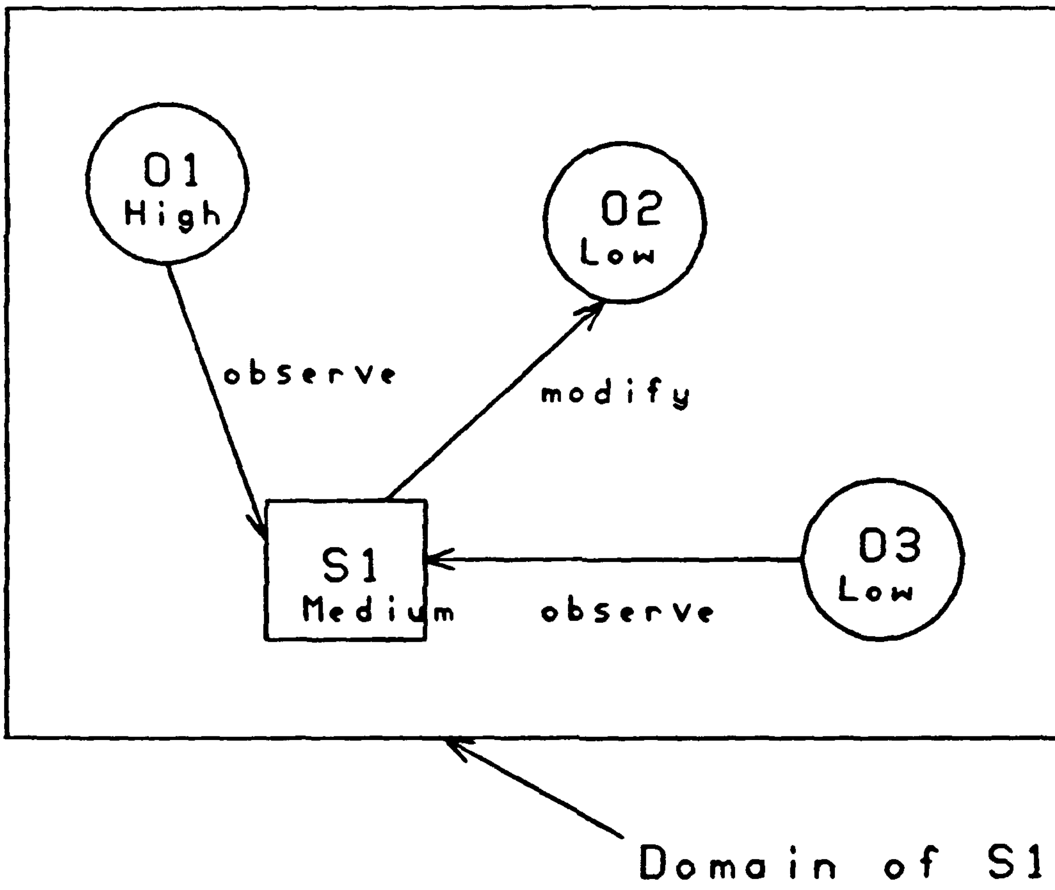


Figure 2 Ring policy

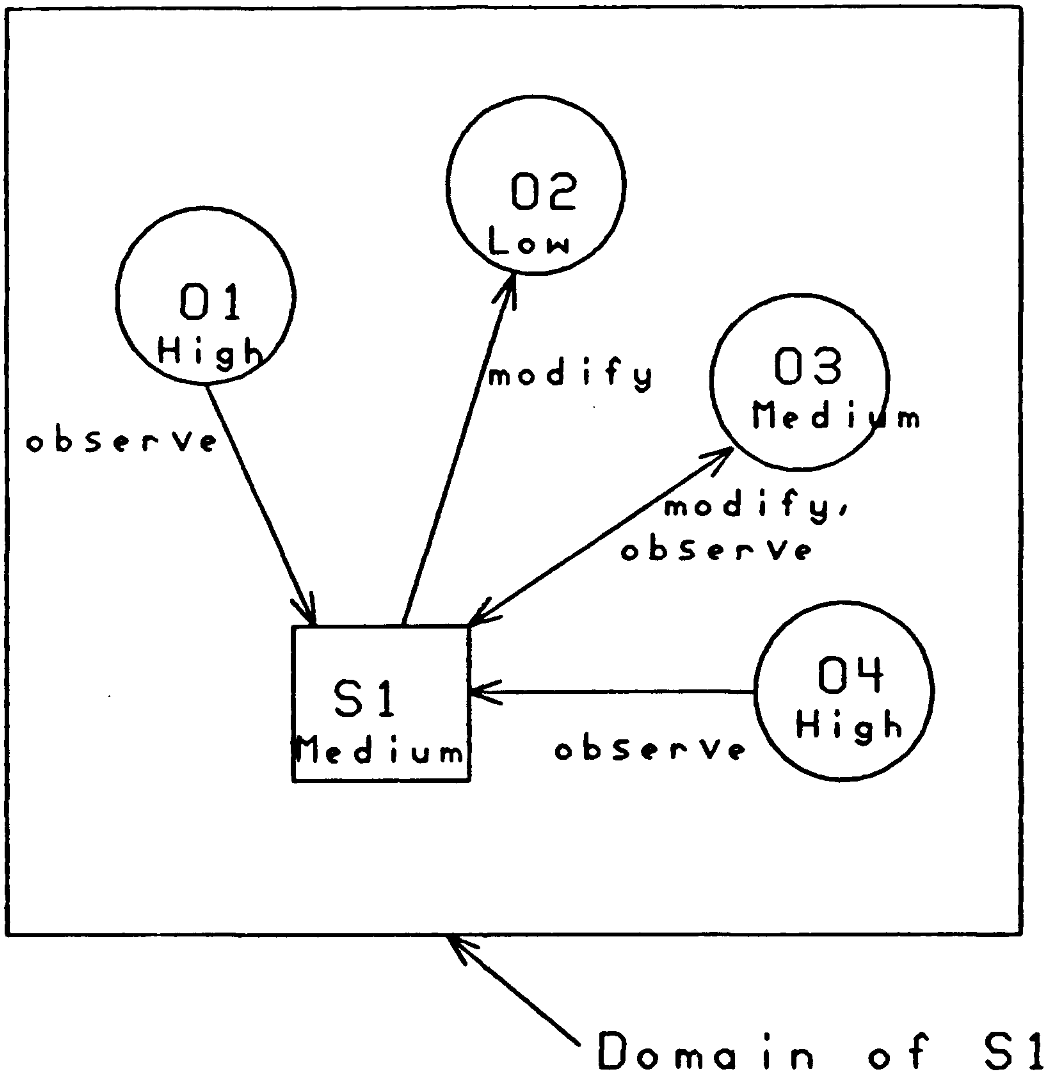


Figure 3   Strict Integrity Policy

2. Discretionary Integrity Policies

Discretionary controls can be modified by a user, or group of users, who is placed on an authorization list which specifies the ability to alter discretionary controls. A user has the ability to define his own integrity controls after access to an object is made, thereby making the controls discretionary. Two discretionary policies discussed by Biba are Access Control Lists and Rings.

a. *Access Control Lists (ACL)*

An access control list is a defined set of subjects that are authorized to access a specific object. Each object within the system has its own access control list. This mechanism is discretionary because the list of subjects can be modified by an authorized user. Certain users, such as system administrators, have the authorization to dictate which subjects are allowed access to which objects. This is based on the present integrity levels of both the subjects and the objects.

The use of access control lists creates the problem of identifying those subjects that are authorized to modify the ACL. This problem can be solved by externally defining those subjects with modification authority and maintaining this list of authorized subjects at a minimum level. Fewer subjects with modification authority means less opportunity for either inadvertant or malicious sabotage.

Figure 4 illustrates the use of an access control list to enforce integrity constraints. Subject S1 has the ability to observe and modify objects which are within its domain, specifically O1 and O2. This is allowed because the ACL for O1 contains S1. The ACL for O2 contains both S1 and S2 thereby authorizing each of the subjects access. O3 has an ACL which contains S2. Each object can be accessed only by those subjects that are contained within their access control list.

b. Rings

The ring policy described here is similar to the ring policy used in mandatory controls with the exception that the access privileges of subjects can be modified. The integrity of objects is protected by allowing modification only by subjects within a specified integrity ring.

Figure 5 illustrates the use of rings. A ring (domain) is established for each subject. The subjects can observe or modify only those objects that are within their respective ring. This figure shows that the rings may overlap as O1 is within the rings of both S1 and S2. Objects that are outside a subject's ring are not accessable by that subject.

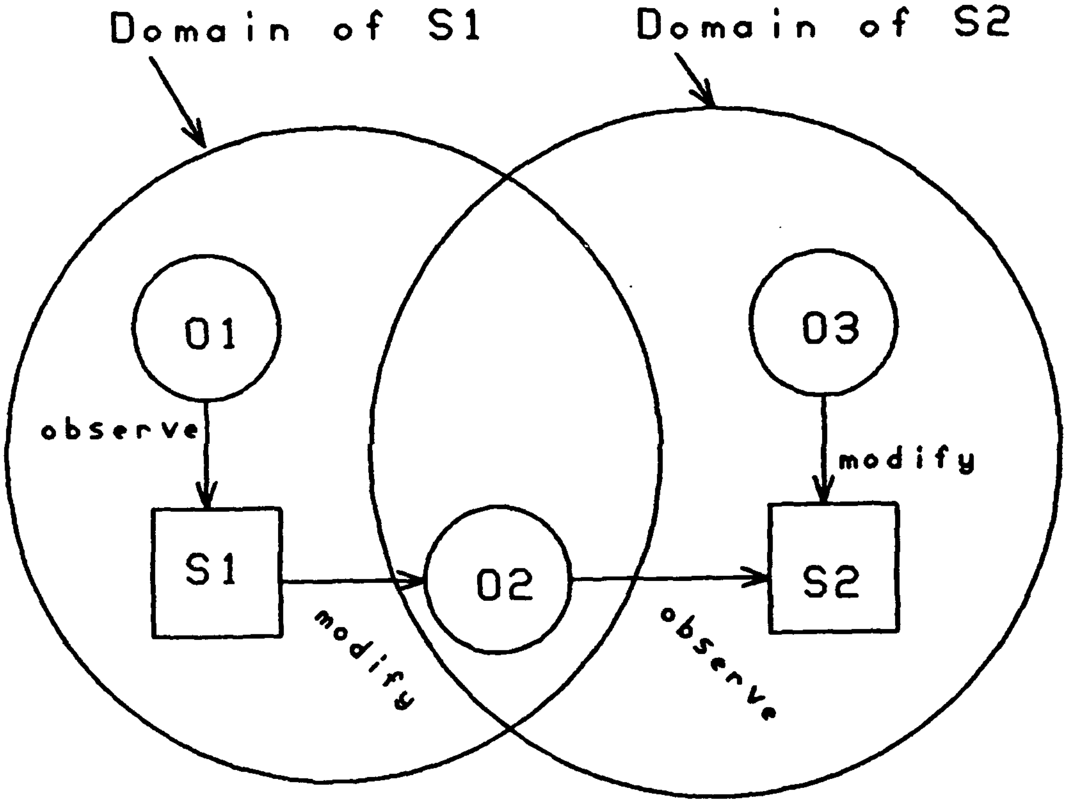


Figure 4 Access Control Lists

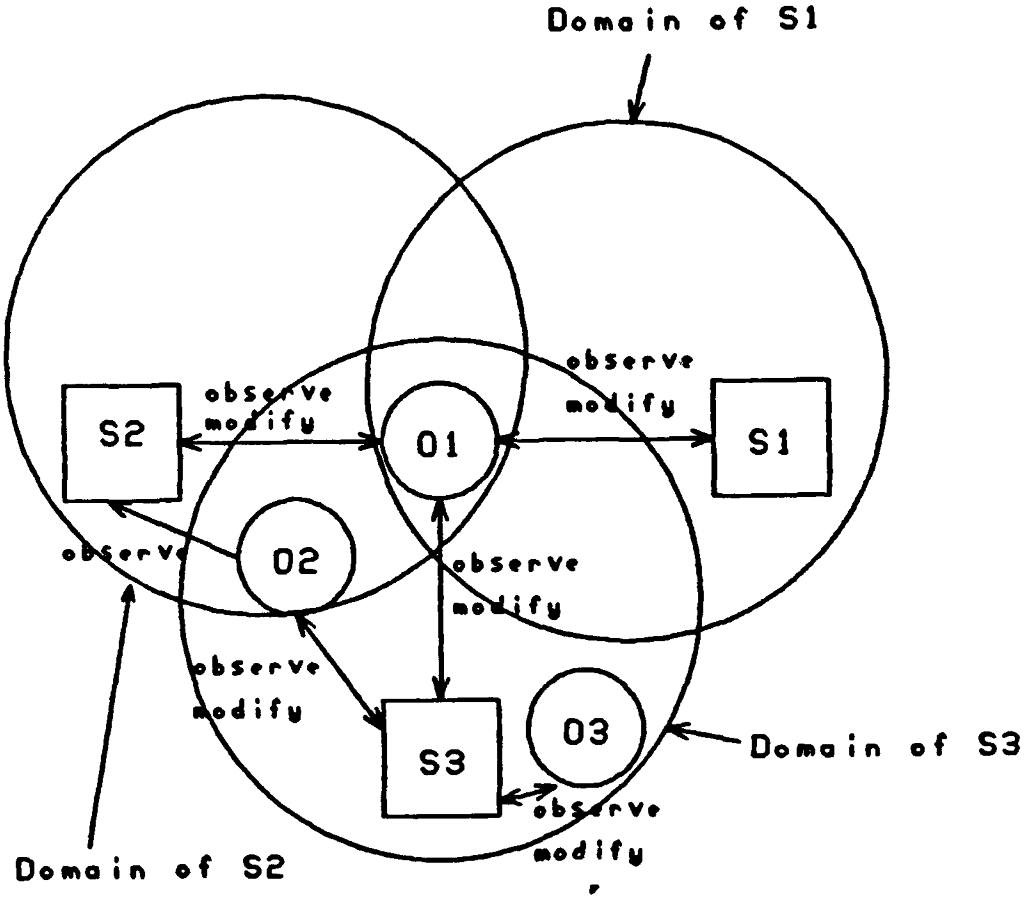


Figure 5 Rings

D. STRENGTHS

A first strength of the Biba model is that it was the first attempt to identify integrity as the dual of secrecy. Biba takes the Bell-LaPadula Model, which is concerned with the unauthorized disclosure of information, and creates a similar model which addresses unauthorized manipulation of information. The Biba model was one of the first models to identify integrity as a topic seperate from secrecy.

A second strength of the Biba model is that it offers a variety of policies for both mandatory and discretionary controls. This variety increases the probability of successful integration of an integrity policy as part of a security plan. Each of the policies has different requirements and specifications which may or may not fit into the design of a security plan. The designer of the plan has more than one option available when deciding on an appropriate integrity policy.

E. WEAKNESSES

The Biba model is designed for implementation in systems featuring ring architecture, especially the Multics' kernel system. The policies are tailored for this system and are not applicable for implementation using anything other than Multics.

While approaching integrity as the dual of secrecy, the Biba model ignores the topic of secrecy. The Bell-LaPadula Model, which is the basis for DOD secrecy policies, does not completely address integrity. Biba attempted to fill this void but has ignored a discussion of secrecy. Formulation of a plan for implementing an integrity policy into a plan for secrecy is needed to create a security policy that can be considered complete.

The policies presented by Biba are not flexible enough for implementation in real-world applications. The policies are not only too Multics specific but are also not capable of being altered to fit into systems that do not meet the specifications for each policy.

Some of the policies presented by Biba have problem areas that make implementation difficult. These problems are mentioned in the sections discussing each policy. Further work is required to correct these deficiencies before the policies can be put into use.

III. GOGUEN AND MESEGUER INTEGRITY MODEL

A. INTRODUCTION

A second data integrity model was presented by Goguen and Meseguer. Their model builds on the concepts of inference control and unwinding. Each of these will be explained separately in this chapter. The model is applicable for a simple multilevel security (MLS) system. A MLS system is one that has different security levels and can prevent users from obtaining information for which they lack authorization [Ref.1:p. 114]. The goal of the model is to verify the MLS system by verifying its internal components. The internal components, or processes, must be capable of meeting the security and integrity requirements of the system. If these internal components do not meet the requirements, then the overall system can not function in a secure state.

B. DEFINITION OF INTEGRITY

The definition of integrity applied by Goguen and Meseguer is based on the idea that there are certain operations, or processes, that are performed on data that must be invisible to certain users. Integrity of the system is maintained if processes do not allow viewers to infer anything about the data by observing the process itself. Integrity is maintained through the use of non-infering processes.

This explains how integrity is maintained but it does not define the authors' idea of integrity. There is no clear definition by the authors of how they view integrity. The most appropriate definition of integrity for application of Goguen and Meseguer's framework is the traditional integrity definition, which is that the data is free from unauthorized manipulation and can be modified only by authorized processes. There is likewise no definition of integrity offered by the authors in their 1982 article [Ref. 7].

C. DESCRIPTION

Goguen and Meseguer have designed their model for application in a multilevel security (MLS) environment. They use two approaches for maintaining integrity: unwinding and inference control. These approaches will be examined separately in this section.

1. Unwinding

The authors view multilevel security as existing in three levels of abstraction. This view is helpful in establishing a definition for the term "unwinding". Progression from one level to another level is accomplished through the process of unwinding. Unwinding leads from one level of abstraction to another with the requirements for proof of the integrity policy becoming increasingly more general rather than specific. Each step of the unwinding process goes further away from human intuition and serves to verify the ideas and constraints of the previous level. This unwinding is a logical progression and ensures a security and integrity policy that is both accurate and complete. In the context of the authors' model, the term security policy refers to a complete policy that encompasses both disclosure control and integrity concerns.

The first level of abstraction in a multilevel security system is the precise statement of the security policy that is to be implemented. This level is closest to human intuition and is a direct expression of the constraints that the security policy needs to enforce. The authors state that this level is the actual expression of the security policy.

The second level of abstraction is obtained by using the authors' unwinding theory to remove the security policy one step away from human intuition. This level consists of the statement of general conditions that must be met by the security policy. The authors write that this hopefully reduces the proof of the policy to simpler conditions and makes guaranteeing the correctness of the policy easier.

The third level of abstraction is the most removed from intuition. This level consists of the statement of a finite set of lemmas, or assumptions, that are obtained by analyzing the specifications of the security policy. The assumptions are used as verification that any system is multilevel secure. If all of the assumptions are true than any system that meets the specifications established by the assumptions is guaranteed to be multilevel secure. This level is based on the idea that if the assumptions are derived through a logically sound procedure, then the problem of proving certainty for any system that meets the assumptions is greatly reduced. This is designed to reduce the requirement for rigorous mathematical proof of system completeness and certainty.

While unwinding can be applied to any security policy the authors demonstrate the application of this technique within the MLS environment. They include in their article a detailed description of each level of abstraction with a MLS security policy. The final result reached by the authors in the MLS case is that unwinding is the formulation of simple conditional equations that describe "the effects of operations on the basic data structures that underlie the system" [Ref.5:p. 81]. Verification of these data structures against specifications by algebraic definitions leads to verification of the entire system.

2. Inference Control

Inference control is preventing high-level classified information from being inferred by combining data at a lower classification level. The authors design their model to prevent users from violating a security policy by an aggregation of data. This is done by defining and establishing boundaries for a logical system and then defining inference relationships that exist between the entities within the system.

Each process within the logical system has a view of the entire system and, in some cases, the process may have a subview. This view is simply the components of the system that a process accesses, or sees. Each process uses data at appropriate integrity levels and is certified to be valid by mathematical proofs. The user, or operator, of the process should possess an appropriate security level clearance to match the classification level of the working data. The view afforded by the process needs to be based on a least privilege concept in that the process should see only that which is essential for proper functioning. The least privilege concept states that the view afforded each process should be large enough to allow functionality while being small enough to prevent unauthorized data from being accessed. Assignment of a limited view to each process will reduce the possibility of inference of high-level data from lower level data.

Similar to unwinding, the authors go through a rigorous proof for inference control in a MLS environment. They define a logical system and apply rules and constraints to enforce inference control. The final result of the authors' work in the MLS example is that inference control can be attained within a relatively simple environment but there does not exist a standard technique that can be applied to more complex security environments. Inference control is difficult to attain in complex systems and requires a great deal of effort with no guarantee of success.

D. STRENGTHS

A first strength of the Goguen and Meseguer model is that it addresses two areas that were not addressed by either Clark/Wilson or Biba. The authors provide two specific measures for ensuring data integrity rather than providing a general approach to the entire system.

A second strength of this model is that it is designed for application in an MLS environment, which is the traditional military standard for security policies. Both unwinding and inference control are designed for implementation within MLS. This offers the advantage of having available a working system for implementation if it is needed.

A third strength of Goguen and Meseguer is that the authors have developed rigorous proofs for both unwinding and inference control. The proofs are presented along with the assumptions, or lemmas, to provide for verification and completeness of the authors' policies.

E. WEAKNESSES

The Goguen and Meseguer article has two weaknesses that can hinder its acceptance and eventual implementation.

A first weakness is the lack of a definition of integrity to be applied to the unwinding and inference control approaches. The concepts of how to maintain security and integrity are throughly presented but a statement of what integrity means should be included. The reader must apply his own definition of integrity to the article. The authors of the two previous models, Clark/Wilson and Biba, present definitions of integrity in their articles. These authors see integrity in different ways and apply their respective definitions to their model. Goguen and Meseguer fail to supply their view of what integrity actually is.

A second weakness is the degree of difficulty and complexity involved in presenting the two concepts developed in the article. The detailed and complete proofs mentioned above as a strength may likewise be labelled a weakness. The article relies heavily on work previously presented by the authors in 1982 and which is almost required reading in order to understand the concepts presented in the article.

IV. CLARK\WILSON INTEGRITY MODEL

A. INTRODUCTION

The Clark\Wilson Integrity Model makes a comparison between military and commercial security policies and takes the findings of this comparison to formulate a model that can be used to preserve data integrity. The authors clearly distinguish between the needs of the military and commercial environments concerning data integrity and use the Department of Defense Trusted Computer System Evaluation Criteria (Orange book) [Ref. 1] to set standards for their model.

B. DEFINITION OF INTEGRITY

Clark and Wilson define "data integrity" as data that is free from unauthorized manipulation and is in a valid state. Free from manipulation means that users, auchorized or unauthorized, have not altered the data in any way. This concept can be expanded even further to say that users do not have the ability to alter the data.

The concept of validity will be discussed in detail later but, briefly, it means that the data is in the same unaltered condition that it was in when it was received. The separation of duties and well-formed transaction mechanisms are used to ensure this validity. The Clark\Wilson model builds on the differences between military and commercial policies and applies the definition of integrity just given to develop their model.

C. DESCRIPTION

The Clark\Wilson Integri^ty Model is built on the premise that ensuring integrity is a two-part process. The two parts of this process are certification and enforcement. Both of these terms are used in reference to data that must be protected against manipulation. The formulation of constrained data items (CDIs), integrity verification procedures (IVPs), and transformation procedures (TPs) provides the basis for establishing rules for developing and implementing the model.

The Clark\Wilson Model begins by identifying Constrained Data Items (CDIs). A Constrained Data Item is a data item which needs to be covered by the model. It is a data item to which the model is applied. Verification that the CDIs are within the constraints of the data integrity model is accomplished by Integrity Verification Procedures, or IVPs. The IVPs ensure that the data is in a valid state before any operations are performed with the data. Transformation Procedures (TPs) are those procedures that move CDIs between valid states. They are used to change the collection of CDIs that correspond to each valid state. Moving from one valid state to another valid state will change the applicable CDIs and this change is performed by a TP or set of TPs. The TP is used in the sense of a well-formed transaction in a commercial integrity model. By allowing only TPs to change CDIs, the integrity of each CDI is ensured .

The term constrained data item is derived from the requirement that only a TP can alter the data. When the CDIs meet the requirements of the integrity policy then a condition known as a "valid state" arises. CDIs will be continuously in a valid state if they are altered only by TPs. The TPs take the CDIs from one valid state to another and thereby maintain data integrity.

Enforcement of the requirement that only TPs manipulate CDIs can by accomplished by the system. The validity of the initial IVP, which confirmed that the CDIs met the integrity policy requirements, and the validity of the TPs can only be accomplished by a trusted user (i.e. security officer). This verification is done by comparing the IVP and each TP against the integrity policy that is in use. This two-step process is the basis of the Clark\Wilson Model. Enforcement of the TP requirement by the system and certific ion of each TP by the security officer are the two steps in the model.

Clark\Wilson develops a set of rules for both the certification and enforcement requirements. These rules are presented below.

There are five rules concerning certification and four rules concerning enforcement. Certification rules are labelled C1 - C5 and enforcement rules are labelled E1 - E4. These rules are given in order of implementation.

(C1): IVPs are required to ensure that all CDIs are in valid states when an IVP is executed.

(C2): All TPs must be able to take a CDI from one valid state to another valid state thereby ensuring integrity of the CDI.

(E1): The system must ensure that only TPs are allowed to manipulate CDIs. Also, there needs to be a relationship created which identifies a user with the TPs that are available for that user as well as the CDIs that the TPs are allowed to access.

These three rules are concerned with the internal consistency of the CDIs. The requirements specified by these rules are met by the proper functioning of the system. Enforcement is also accomplished by the system.

(E2): The relations developed in E1 must be stored by the system so that users are only capable of accessing those TPs for which they are authorized.

(C3): The relations that are created by E1 and stored by the system in E2 must meet the requirements of the integrity policy.

(E3): The system must be capable of capturing the identification of each user and verifying that the user is allowed to use only those TPs for which he is cleared.

These rules develop the requirement for each user to be identified upon initial access to the system so that only appropriate TPs are available. This limits access to TPs and therefore, CDIs to authorized users.

(C4): All TPs must be capable of writing to a write-only CDI the information that is necessary to reconstruct the TP if required. This creates a "log" to record the occurrence of each TP as well as the design of the TP itself.

Rule C4 establishes an audit trail for each TP. Pertinent information about each TP is captured so that independent reconstruction of the TP is possible. This creates a log to serve as a document for audit.

The next rule (C5) addresses a component of the model that has not been previously mentioned. This component is the Unconstrained Data Item, or UDI. An Unconstrained Data Item is a data item which is not covered by the integrity model. UDIs are important because they represent the most common method for entering new data into the system. The authors give the example of a user typing information at a keyboard. This shows that a TP can accept unconstrained data as input and then alter the value of certain CDIs based on these UDIs. Rule C5 is necessary to provide for certification of UDIs.

(C5): A TP must be capable of taking a UDI as input and transforming that UDI into a valid state CDI. If this can not be done then the UDI must be rejected by the TP.

The final rule (E4) prevents a user from creating a TP and then executing that TP without any certification taking place. Enforcement of this rule prevents bypassing the certification requirements.

(E4): An individual with the ability to certify IVPs or TPs must not be capable of executing those same IVPs or TPs.

The combination of these rules forms the basis of the system. The enforcement rules, which the authors correspond to the application-independent security functions, and the certification rules, which correspond to application-specific definitions for integrity, define the system. The authors desire to place as much responsibility as possible on the enforcement rules thereby limiting the certification requirements. This is desireable because of the complexity of the certification process compared to the enforcement capability of the system.

D. STRENGTHS

Clark\Wilson has been acknowledged as a new approach to defining and maintaining data integrity. There has been a great deal of follow-on work which takes the basics of Clark\Wilson and attempts to refine the model for implementation with specific computer systems. This follow-on work has served to highlight some of the strengths of the model. These strengths are presented below.

The definition of integrity used in Clark\Wilson relates to integrity as a concept within the context of a computer system. Their model offers a working definition that is applied effectively to the area of computer data. The model supports the definition offered and builds a framework that is targeted at maintaining integrity within the scope of the authors' definition.

A second advantage of Clark\Wilson is that it identifies the features of a computer system in which integrity is the main goal. The model provides a blueprint for basic rules that must be established and implemented in systems that are used to maintain integrity. Adherence to the rules established in the model will allow the construction of a valid, working integrity mechanism.

A third strength of Clark\Wilson is that it can be used to expand the Department of Defense Orange Book security model to cover the topic of integrity as well as control of classified data. The model has potential for implementation within DOD systems if it is adopted under the guidelines of the Orange Book. The model can be used to compliment the security model constructed by the Orange Book.

A fourth strength of Clark\Wilson is its applicability to the non-DoD environment. This model is easily understood by the commercial world and has the potential for commercial applications as well as DoD applications.

E. WEAKNESSES

There are several criticisms concerning weaknesses in the Clark\Wilson Model. The following three areas show the most significant weaknesses that have been detected by critics.

A first weakness of the Clark\Wilson Model is its inability to have the integrity controls strictly internal [Ref. 8:p. 1-7]. The dual process of certification and enforcement takes into account both the environment internal and external to the system. The enforcement is accomplished internally by the system itself while the certification is performed externally by a security officer. This means that the system will maintain the integrity of data that has been verified externally before being entered. The system may accept data that has been entered incorrectly by either accidental or malicious means. External verification declares the data to be in a valid state. The system accepts the data and maintains its integrity. There is not a mechanism within the system to check the correctness of the data that has been input. Certification and enforcement are not both internal to the system.

A second weakness of the Clark\Wilson Model is that, by requiring IVPs, the model needlessly complicates the certification process. As mentioned earlier, it is desirable to shift as much of the verification responsibility to enforcement because enforcement can be done by the system. Since an IVP is essentially a special type of TP the requirement for IVPs is redundant [Ref. 8]. This redundancy contrasts to the authors desire to use minimal certification rules because of the level of complexity and the manual work necessary for certification.

A third weakness of Clark\Wilson is that it is applicable only at a single level of granularity, which is the size and resolution of the protected system elements [Ref. 9:p. 270]. The author of [Ref. 9] has developed rules concerning integrity policies and how they relate to the level of granularity. The dominant rule developed is that at each level of granularity, the integrity policy should specify how the state may change in terms of the next lower level of granularity. As it is presented, Clark\Wilson is designed for use at a single granularity level. The inability of the model to be implemented in a multi-granular environment limits its range of applicability.

V. A FRAMEWORK FOR COMPARISON

A. INTRODUCTION

This chapter establishes a framework for comparing the data integrity models. The framework is fully developed and justified before being applied in Chapter VI. It is designed so that each model can be evaluated individually with the results being used to make recommendations concerning the suitability of the respective model for DoD applications. In Chapter 6 this framework is applied to the three models presented in the earlier chapters to determine whether the Clark/Wilson, Biba, or Goguen and Meseguer data integrity models should be adopted as a formal standard.

B. FRAMEWORK DESCRIPTION

The framework provides a means for comparing the models on a common basis. Since each model addresses data integrity from its own unique approach, establishment of a common ground is based on generic, rather than specific, areas. The areas examined in the framework are:

1. The definition of integrity used in the model.
2. Concepts on which the model is based.
3. Suitability of the model for DoD applications.
4. Advantages and limitations of model.

The proposed framework is presented in Figure 6.

1. Definition of Integrity Used in Model
    - Adequacy/Completeness
    - Assumptions
2. Concepts on Which Model is Based
    - Central theme
    - Relation to Secrecy
3. Suitability for DoD Applications
    - Characteristics of DoD Environment
    - Relationship of Model to DoD Environment
4. Advantages and Limitations
    - Description of Strengths and Weaknesses
    - Correction of Deficient Areas

Figure 6

1. Definition of Integrity Used in Model

a. Adequacy/Completeness

This area of analysis addresses the question of whether the definition of integrity used in the model is complete and adequate. This question cannot be answered until a common definition of integrity is offered as a standard by which each model's definition can be measured. Of many existing definitions [Ref. 8], the definition that was developed by the Integrity Working Group (IWG) of the Invitational Workshop on Data Integrity [Ref. 8:p. A.1-2] seems to best serve as a standard. This definition is:

> Integrity - a property that data, an information process, computer equipment and/or software, people, etc. or any collection of these entities meet an a priori expectation of quality that is satisfactory and adequate in some circumstance. The attributes of quality can be general in nature and implied by the context of the discussion; or specific and in terms of some intended usage or application.

This definition was selected as the standard for comparison because of both its flexibility and its completeness. It addresses many aspects that are commonly associated with the notion of data integrity while remaining broad enough to be applied to many environments.

A closer examination of this definition shows that it can be broken down into the following key elements:

(1) "data, an information process, computer equipment and/or software, people, etc. or any collection of these entities." This prevents the restriction of the definition to data integrity alone. This broadness makes this specific definition a good tool for comparison as many different aspects of integrity are addressed. The axiom here is that the broader the standard, the greater the number of definitions that can be measured against it.

(2) "a priori expectation". This term emphasizes that there must be a goal or desired outcome (i.e. expectation) for the element being studied for integrity. The outcome is based on theory instead of experience or experiment.

(3) "quality". This term refers to the attributes that characterize the element being studied. The most common attributes contained within the heading of quality are accuracy, timeliness, consistency, and completeness. Robert Jueneman [Ref. 8:p. A.5-14] states that integrity is not quality but rather it is the "extent to which the qualities (i.e., accuracy, precision, timeliness, etc.) taken together are considered adequate for a given purpose."

The definition of integrity offered as a standard will be used to measure the appropriateness of the definitions developed in the three data integrity models described in earlier chapters. In this situation, appropriateness is dependent on, and equated to, completeness. The completeness of each definition is concerned with the aspects of integrity that are addressed. It is not practical to expect every existing definition of integrity to address all aspects covered by the standard. Each definition must be evaluated for completeness within the environment in which it is employed as well as against the IWG standard.

Evaluating for completeness will highlight the aspects of integrity that are addressed and, more importantly, those aspects that are ignored. This will be useful when determining whether the model that uses the definition is suitable for DoD applications. The consequences of an incomplete integrity model can be assessed before acceptance and implementation of the model.

b. Assumptions

When evaluating the integrity definitions in the three models it is necessary to determine the assumptions, if any, that the author(s) make. Assumptions can be made concerning a great number of areas and, unfortunately, can create a void that can hinder eventual acceptance of the model. Each model will be examined for the assumptions that it makes concerning its definition of integrity. The validity of each assumption needs to be evaluated so that there are no areas lacking support.

2. Concepts on which Model is Based

This section of the framework addresses two specific questions:

(1) What is the central theme on which the model is based?

(2) Is there any relation between the model and secrecy?

a. Central Theme

The central theme of the model is important as it will be useful in determining compatibility with DoD applications. The basic theme of each model should be based on sound, provable principles that make the model practical instead of simply theoretical.

Clark\Wilson builds on the premise of separation of duties and well-formed transactions. The validity of this premise will be evaluated for possible areas of omission or conflict. Biba uses the "no read-up, no write-down" concept; Goguen and Meseguer employ as a basis the concepts of unwinding and inference control. These models will likewise be evaluated for areas of omission and conflict.

A thorough evaluation of each model's basic concepts is necessary before a decision can be made concerning acceptance and implementation. Schell [Ref. 10:p. 89] points out that the first step in planning any security system, whether it addresses disclosure and manipulation together or simply disclosure alone, is the ability to identify what the system needs to protect. If the object requiring protection is identified then a plan can be formulated concerning how to provide the needed protection. This is the phase where knowledge of the perspective models and their functioning plays a key role. The question of whether a specific model is appropriate can be answered accurately [illegible] the model is studied and understood.

b. Relation to Secrecy

The second question to be answered in this section concerns the relationship between the data integrity model and secrecy. This issue is important because of the possible incorporation of the model into a complete security policy that addresses both disclosure and manipulation. The TCSEC [Ref. 1] does not address manipulation of data and therefore can be considered somewhat incomplete. Because the TCSEC does not address integrity it is not possible to produce a "laundry list" of requirements that a data integrity model should meet. The TCSEC addresses confidentiality, which is the primary concern in handling classified information. Once this problem has been adequately addressed, emphasis turns to the problem of controlling unclassified information. This is where the issue of data integrity is a primary concern [Ref. 8]. For completeness, the TCSEC needs to be updated to provide guidance for protecting data from manipulation and thereby preserving the integrity of the data.

An examination of the three data integrity models in this thesis and their relationship to secrecy will determine whether they can possibly be incorporated into the TCSEC to fill the existing void.

3. Suitability for DoD Applications

This section of the framework examines the applicability of each data integrity model for a DoD environment. This is accomplished by first describing the specifics of a DoD environment and then testing each model for its goodness of fit to these specifics.

a. *Characteristics of a Military Environment/ Relationship to Model*

A DoD environment is synonymous with a military environment, which is the more common terminology. Military environments are primarily concerned with the protection of classified data from unauthorized disclosure. Only recently has attention been directed to the issue of protection from manipulation.

The difference between a military environment and commercial, or private, environment is in the goal of their respective security systems. The military viewpoint is that controlling access to data, specifically read access, is the foremost goal of any security system. The commercial viewpoint differs from the military viewpoint in that the emphasis is not on access to data but on prevention of data alteration. This commercial viewpoint stresses integrity, not secrecy [Ref. 11:p. 73]. The specifics of a DoD environment dictate that a data integrity model be capable of implementation within a multi-level security system. Disclosure rules will separate data into different classifications. Individual users authorized to access classified data must be restricted in their capability to modify that data. There need to be modification constraints established at each classification level for each user. The model should be able to attach integrity labels that are similar to already existing classification labels.

b. Relationship of Model to Military Environment

This area examines the ability of the model to attach the proper integrity labels discussed above. The model need not be restricted to the labels already in use in the military security classification system (i.e. Confidential, Secret, and Top Secret). Rather, the model must be capable of attaching its own labeling scheme. The key point is that the model can properly label data which reside at different integrity levels, thereby restricting the operations that can be performed on or with that data.

4. Advantages and Limitations

The advantages and limitations of each data integrity model must be evaluated and understood before selecting a model for implementation. This section will look at the advantages and limitations discussed for each model in their respective chapters. An examination of these areas will help to answer the following questions:

(1) Will the weakness of the model prohibit acceptance?

(2) Can areas of weakness be corrected or modified to make the model acceptable for DoD applications?

a. Description of Strengths and Weaknesses

The strengths of each model are important for performing an analysis of benefits to be achieved by accepting the model. This will determine what voids in the current security policy the model can fill.

While noting strengths is important, the emphasis in this section is on limitations. This is because the limitations of each model will be the deciding factor in determining whether the model can be accepted and implemented as a standard.

The limitations of each model will be examined for the reasons given above. If the model has limitations that make it unacceptable and these limitations cannot be corrected, then the model will be inappropriate regardless of its strengths. If the limitations can be corrected then the model can be considered for acceptance.

b. Correction of Deficient Areas

This section examines the noted weaknesses of the model and attempts to determine whether these weaknesses can be corrected. The decision must be made concerning acceptance based on a thorough evaluation of the model's weaknesses. If the weaknesses cannot be overcome then the options available to the decision maker are limited. The option of accepting the model with modification is eliminated. If corrections can be made, then analysis of the feasability of making these corrections must be done. The corrections may involve processes which excessively complicate the model and actually create another weakness while solving the original weakness.

C. FRAMEWORK APPLICATION

The framework developed in this chapter will be used to analyze each of the three data integrity models. The goal of the framework is to provide a means for comparing the models on a common basis. This comparison will be made in Chapter VI.

After applying the framework to the models, recommendations concerning acceptance can be formulated. These recommendations will form the basis for the selection decision.

VI. MODEL COMPARISON

A. INTRODUCTION

In this chapter, the framework developed in Chapter V is applied to the Biba, Goguen and Meseguer, and Clark\Wilson data integrity models. Each model is evaluated in the four areas of the framework for the purpose of making recommendations concerning suitability for DoD applications. The models are evaluated simultaneously with each area being examined before moving on to the next area.

B. MODEL COMPARISON

1. Definition of Integrity Used in Model

The definition of integrity used in each model is examined for the purpose of determining its adequacy, completeness, and assumptions. The definitions are measured against the standard set by the definition which has been adopted as a benchmark, namely the Integrity Working Group (IWG) definition presented in Chapter '.

Before examining each definition it is helpful to restate the appropriate definition for each model as developed in the respective chapter. These definitions are:

> Biba: integrity is a system property which guarantees that a system or subsystem will perform as intended by its creator.

Goguen and Meseguer: integrity is based on the idea that there are certain operations that are performed on data that must be invisible from users. Integrity, a property, is maintained if users are unable to infer anything about the data by observing the processes involving the data. This is based on the underlying idea that data possesses the property of integrity if it is free from unauthorized manipulation and can be modified only by authorized processes.

Clark\Wilson: integrity is a property assigned to data that is free from unauthorized manipulation and is in a valid state.

a. *Adequacy*

Adequacy, as stated in the IWG standard, is concerned with the areas of integrity that are addressed by the definition. Adequacy is strongly related to the idea of completeness. The IWG standard definition itself is both adequate and complete as it addresses many of the areas frequently associated with data integrity. Analysis of the three models produces the following results:

(1) Biba. The Biba definition treats integrity as a relative measure rather than an absolute. There is no a priori statement concerning the performance specifications of the system. Rather, the system need only perform to the designer's intent, whatever that intent may be [Ref.12:p.60].

This perspective makes the Biba definition extremely broad. It places the responsibility for integrity on the ability of the creator to design a system in which integrity can actually be achieved. Because of this, the Biba definition is lacking in specific detail and is general enough to be applied to almost any system or subsystem. Flexibility is present; standardization is missing. The conclusion from this is that the Biba definition of integrity is adequate but not complete.

(2) Goguen and Meseguer. The integrity definition offered in the Goguen and Meseguer model addresses noninference. This refers to the ability of the system to "hide" the data from users working with certain processes. If a user cannot infer anything about the data from the process, then the system is said to have integrity. This definition addresses neither the process nor the qualities of the data in detail. There is an a priori expectation of what should happen, specifically that the user should not be able to gain knowledge from inference.

The Goguen and Meseguer definition is both adequate and complete when applied in the appropriate context. A system that has the ability to separate its objects from its subjects is the most appropriate situation for application of this definition. If, however, the system does not have this capability, then Goguen and Meseguer' definition is not well-suited for implementation.

(3) Clark\Wilson. The Clark\Wilson integrity definition is based on prevention of unauthorized manipulation of data. Data that is in a valid state is maintained in that valid state, thereby ensuring integrity, only if authorized manipulations are performed on or with the data. This definition is broad enough to be applied to many different environments. There is no method addressed for determining whether the data is initially in a valid state. The valid state concept serves to isolate the data and label it as being worthy of protection. This is essential in setting limits to the items that need protection.

The definition used in Clark\Wilson is the most useful of the three models because of its applicability to many types of environments. This definition is complete in respect to the IWG standard and as a result is quite adequate.

The conclusion reached in this section is that the Biba ana Clark\Wilson integrity definitions are adequate in accordance with the IWG standard. The Goguen and Meseguer definition is contextually dependent concerning adequacy.

b. Assumptions

The assumptions made concerning the integrity definition in each model are analyzed to determine if the definition is realistic. This is to check the relacion of the definition to the real world. Assumptions may be so great that they make the integrity definition, and possibly the entire model, potentially unacceptable for implementation in any environment. Because of this, caution should be exercised when making assumptions to accompany any data integrity definition. Analysis of the three data integrity models follows.

(1) Biba. The assumptions made in the Biba definition are:

(1) The system being evaluated is designed in such a way that integrity can actually be achieved.

(2) There has been an external verification performed on the system to ensure that it is functioning properly.

(3) Classification labels exist for integrity levels. These classification labels are quite similar to the levels attached to the security classifications used for military information.

Each *of* these assumptions is based on sound reasoning. The design of the system is irrelevant from the Biba model perspective. Likewise, the external verification is a realistic condition to expect before implementation of integrity controls. The existence of integrity classification labels is quite necessary and is not an unreasonable expectation. The conclusion after examining these assumptions is that the Biba definition does not stand on insupportable assumptions and that each of the assumptions is both necessary and reasonable.

(2) Goguen and Meseguer. There is only one assumption made concerning the integrity definition used in this model. This assumption is that the processes that users can execute have been verified to be properly functioning. A properly functioning process will not allow inference and therefore will maintain the integrity of the data involved in the process.

The assumption made concerning the definition in this model is similar to the assumption made in the Biba definition. Just as in Biba, this is a reasonable assumption and does not make the integrity definition unacceptable.

(3) Clark\Wilson. The Clark\Wilson integrity definition incorporates three assumptions. These are:

(1) Data is initially received in a valid state. There is no mechanism available within the model to test for validity, it is simply assumed.

(2) The initial Integrity Verification Procedure (IVP), which confirms that the data items requiring protection meet

certain conditions, is assumed to be a valid process itself.

(3) It is assumed that the data item and the real world object that it represents correspond closely.

Each of these assumptions is acceptable with the possible exception of the assumption concerning the integrity of data upon its receipt. The assumption that data is in a valid state, specifically that it is correct and in its original form, creates a precondition that is not easily met. It is somewhat unrealistic to assume that all data is received in a correct state. Many things can happen to data to change either its format or content. Designing a system based on an integrity definition that requires received data to be in a valid state is probably not the best approach to addressing the data integrity problem.

The conclusion in this area of analysis is that each of the models is based on sound, reasonable assumptions that do not damage the model's credibility. The necessary assumptions are not liabilities for any of the models.

2. Concepts on which Model is Based

This section examines the central theme of the model and the relation of the model to secrecy. This is useful in helping to determine compatibility with DoD objectives.

a. *Central Theme*

The central theme of the model is important as it will be useful in determining compatibility with DoD requirements. It also serves to determine whether the model is practical or simply theoretical.

(1) Biba. The central theme of the Biba model is the development of a hierarchical lattice which is used to identify authorized users and also separate users by type [Ref. 12:p.57]. This allows Biba to implement his "no read-up, no write-down" restrictions. This system is effective in preventing modifications by unauthorized individuals.

Biba implements his "no read-up, no write-down" restriction through the use of both mandatory and discretionary controls, which are described in detail in Chapter II. There are integrity classifications within the model which assign data to different levels. These classification labels can be either military-oriented or commercial-oriented. The use of mandatory and discretionary controls along with the assignment of classification labels support the central theme of this model.

(2) Goguen and Meseguer. The central theme of this model is based on two concepts: inference control and unwinding. The concept of inference, which is described in detail in Chapter III, prohibits users from learning anything about the data from the processes that they execute. This

property places restrictions on the design of the processes that can be used in a system implementing Goguen and Meseguer integrity controls. Processes, whatever their purpose, must be designed with the capability to hide the data that they use. This may not be possible to accomplish for all processes. The interactions of various processes must also be capable of preventing inference to protect the integrity of the data involved in those processes. This condition complicates the design of even the simplest systems.

The second concept used in the Goguen and Meseguer model is unwinding. This is the process of observing an integrity mechanism from different levels of abstraction. This unwinding begins with an examination of the policy to be implemented and then looks at the "larger picture" of the entire system, with each successive step in the unwinding being further removed from intuition. This allows for examination of a specific integrity policy or model with the requirement of proof being focused on increasingly general terms as the unwinding goes further from intuition.

(3) Clark\Wilson. The Clark\Wilson model is built on two premises: the well-formed transaction and separation of duty. A well-formed transaction is designed so that it allows only authorized modifications of data. This transaction will prohibit unauthorized manipulation, thereby preserving the integrity of the data. Just as in the Goguen and Meseguer

model, there is a requirement that the transaction, or process, be designed in such a way that this well-formed label may be applied. This is not a trivial matter, especially in large scale systems.

The second premise in Clark\Wilson is separation of duties. This is necessary to preserve a correspondence between data objects and the real world objects that they represent. This separation prohibits unauthorized manipulation by breaking an operation into several subparts and requiring that each of the subparts be executed by different individuals [Ref. 12:p. 68]. In this way, no one user can execute an entire operation. This will prevent malicious tampering with the data with one exception, namely when there is collusion among users.

The conclusion of this section is that the central theme of the Biba and Clark\Wilson models is largely practical, thereby making implementation possible. The theme of the Goguen and Meseguer model is more theoretical and lacking in implementation detail.

b. Relation to Secrecy

The relation of the data integrity model to secrecy is important as it will be a factor in the decision concerning acceptance for possible incorporation into the Orange Book.

(1) Biba. The Biba model has the strongest relation to secrecy of the three models analyzed. Biba takes the Bell-LaPadula model and creates its dual for integrity. The mechanisms in the Bell-LaPadula model are incorporated in Biba thereby allowing for implementation of both models simultaneously. The requirement for integrity classification labels in Biba is matched perfectly with the security labels developed in Bell-LaPadula. This ties an integrity policy to a security policy, thereby creating a complete protection policy for access control and modification control of data.

(2) Goguen and Meseguer. This model relates to secrecy in that it has as its first step the development of the security policy that is to be implemented. Integrity controls can be a part of this policy. As unwinding takes place, the policy is examined from an increasingly broader viewpoint. Integrity mechanisms can be incorporated into the overall security policy at any level of abstraction. As with security, the integrity mechanisms rely on increasingly more general requirements of proof as unwinding takes place. The ability of the system to prevent inference is an integrity mechanism that has a strong relation to the security of the data. Access to data is controlled by the security policy. The ability to prevent inference is controlled by integrity mechanisms. If an unauthorized user is successful in gaining access to data, then the integrity mechanisms will treat that

user as an authorized user. The distinction between authorized and unauthorized users is not made by the integrity mechanisms. Rather, it is the responsibility of access controls.

(3) Clark\Wilson. Clark\Wilson relates to secrecy in that it has the ability to limit the data that a user can access. This is a method of disclosure control. This model uses separation of duties and well-formed transactions to prevent one user from having the ability to execute all steps of one specific process. This helps to preserve the integrity of the data while at the same time establishing an access control mechanism. Because of this feature, Clark\Wilson has a strong relation to secrecy and also to the requirement for access control that characterizes a secure military system.

The conclusion drawn from the analysis in this area is that the Biba model has the strongest relation to secrecy while the Goguen and Meseguer has the weakest. The Clark\Wilson model is in the middle of the other two models.

3. Suitability for Military Applications

This section examines the applicability of each data integrity model for use in a DoD environment, which is described in Chapter V. The main area examined is the ability of each model to attach proper integrity labels. The labels are not restricted to the existing labels for access control (i.e. Confidential, Secret, and Top Secret). It needs to be noted that there currently does not exist criteria for determining integrity levels [Ref. 12]. Access control labels exist, integrity labels do not.

(1) Biba. Biba's model presents several policies for ensuring data integrity. His model has been designed to be the dual of the Bell-LaPadula model, which is the standard for military security classifications. Specifically, the Strict Integrity Policy introduced by Biba is especially suitable for DoD applications. In this policy, the integrity of both subjects and objects is static and externally defined. This policy uses mandatory controls and is quite similar to the security classifications currently in use in DoD. As such, it is one of the most promising of all integrity policies for implementation within DoD, specifically within the Orange Book.

(2) Goguen and Meseguer. The Goguen and Meseguer model is adaptable to the requirement of integrity labels because of its use of domain separation. This domain separation is similar to the Access Control Lists (ACL) used in Biba's discretionary integrity controls. The term "domain" is used to refer to the grouping of objects that a specific user is allowed to access [Ref. 12:p. 61]. By restricting the available objects, integrity of the system can be preserved. This domain concept can be extended to cover the objects available to a user based on the integrity level of that user.

If the objects possess integrity labels, then access to these objects can be limited to only those users with proper authorization. This is similar to the access control classification system used in the Orange Book. The result of this capability is that the Goguen and Meseguer model has the potential for success in a DoD application.

(3) Clark\Wilson. The Clark\Wilson model recognizes the difference between commercial environments and military environments. The emphasis in commercial environments is on data integrity whereas the emphasis in military environments is on disclosure control. The model is designed with the intent to develop integrity controls for the military environment. As discussed in Chapter V, the term military environment is synonymous with DoD environment. This characteristic of Clark\Wilson makes it extremely compatible with existing DoD requirements and classifications for disclosure. As it is written, Clark\Wilson is not designed to attach integrity labels. The capability to do such labelling would enhance its applicability to DoD environments.

Each of the models has the potential for implementation of an integrity labelling mechanism with the Biba model being the most promising of the three.

4. Advantages and Limitations

The advantages and limitations of each model are analyzed to help in determining suitability for DoD applications.

a. *Description of Strengths and Weaknesses*

The strengths and weaknesses of each model are given in detail in the appropriate chapter. This section highlights the areas that either make the model more acceptable or hinder its acceptance.

(1) Biba. The notable strength of the Biba model is that it is the first attempt to treat integrity as the dual of secrecy. This gives it a high degree of compatibility with military security policies and models. This correspondence allows for integration of Biba, specifically the Strict Integrity Policy, into DoD standards for data protection.

The most limiting weakness of the Biba model is its orientation to systems which feature ring architectures, especially a Multics kernel system. This narrows the number of systems which can implement the policies developed by Biba.

(2) Goguen and Meseguer. This model has as a strength its approach to data integrity. Rather than providing a general approach to an entire system, Goguen and Meseguer provide two specific measures to ensure integrity. These measures are unwinding and inference control. This approach differs from the approach used in both Biba and

Clark\Wilson and it offers procedures to be implemented to ensure integrity.

The limitation of Goguen and Meseguer is that it does not offer an explicit definition of integrity for which the two methods of control can be applied. This creates a void in the area of establishing a goal for the integrity controls. In what state does the data need to be in, or what characteristics does it need to possess in order to be considered as having integrity. These questions cannot be answered without a definition of integrity for the model.

(3) Clark\Wilson. The main strength of the Clark\Wilson model is that it identifies the features of a computer system in which integrity is the main goal. As stated in Chapter IV, the model provides a blueprint which includes basic rules that must be established and implemented in systems that desire to maintain integrity. The model presents nine rules for enforcing integrity and the combination of these rules forms a mechanism that will consistently enforce integrity.

The most limiting weakness of Clark\Wilson is that its requirement for Integrity Verification Procedures (IVP's) needlessly complicates the certification process. The requirement that all procedures using the data be verified is a necessary but complicated matter. This places a great deal of emphasis on the process of certifying procedures before those procedures are executed and allowed to access the protected data.

b. Correction of Deficient Areas

This is an analysis of the weaknesses noted above for each model and a determination as to whether these weaknesses can be eliminated.

(1) Biba. The noted weakness of Biba is its heavy orientation to ring architecture systems, thereby making the model somewhat inflexible. However, this is not a weakness that renders the model unacceptable for DoD application. The feasibility of application to systems featuring other types of architecture must be determined. The Biba model can be adapted to other architectures without major modifications. The principles of the model are valid for application to any type of system, even though the specific details are not.

(2) Goguen and Meseguer. The lack of an established integrity definition in the Goguen and Meseguer model is a relatively minor limitation. Though the authors do not supply their own definition, there are many possible definitions of data integrity that fit into the context of this model. This is a limitation that has no effect on the possible acceptance of this model as a DoD standard.

(3) Clark\Wilson. The requirement of Clark\Wilson that certification is needed for those procedures that access protected data is its main limitation. This is a limitation

that must be dealt with before acceptance. There is a real need in this model for the procedures to be certified for proper functioning. However, there is an assumption made that the data in the model was received in a valid state and therefore is worthy of protection. This assumption is acceptable for the data but it is not acceptable for the certification of the procedures. This limitation cannot be overcome without having an adverse effect on the proper functioning of the mechanisms in the Clark\Wilson model.

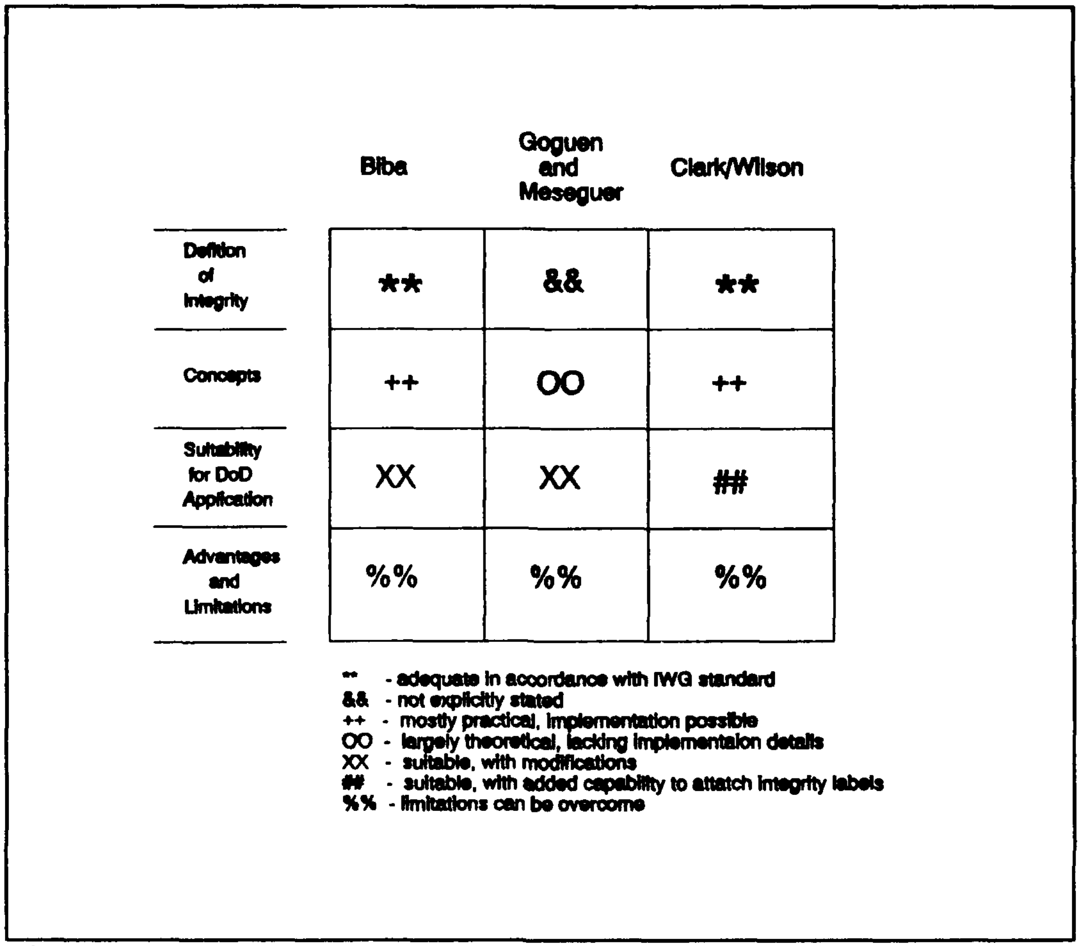
C. CONCLUSION

The framework developed in Chapter V has been applied to the three data integrity models in order to determine their suitability for DoD applications. The models were analyzed in the four areas that constitute the framework with the results shown in Figure 7. This comparison table shows the abilities of each of the models in the four criteria areas.

After completion of the analysis, the following conclusions have been reached:

(1) The Biba data integrity model is based on both an adequate integrity definition and practical concepts. This model is capable of implementation in a ring architecture system, and with modification can be implemented in a DoD environment.

(2) The Goguen and Meseguer data integrity model is based on largely theoretical concepts and lacks a definition



	Biba	Goguen and Meseguer	Clark/Wilson
Defition of Integrity	**	&&	**
Concepts	++	OO	++
Suitability for DoD Application	XX	XX	##
Advantages and Limitations	%%	%%	%%

** - adequate in accordance with IWG standard
&& - not explicitly stated
++ - mostly practical, implementation possible
OO - largely theoretical, lacking implementaion details
XX - suitable, with modifications
- suitable, with added capability to attatch integrity labels
%% - limitations can be overcome

Figure 7 Comparison Table

of integrity for application of the model's controls. However, the model may be accepted for implementation in DoD environments if further '.rk is accomplished to make the model more practical.

(3) The Clark\Wilson data integrity model offers an adequate integrity definition and is based on sound, provable concepts. This model is well-suited for DoD environments . With the added capability of integrity

label attachment, this is the most practical model for acceptance as a DoD standard.

VII. CONCLUSION AND RECOMMENDATIONS

A. CONCLUSION

The analysis performed in chapter VI allows for recommendations to be made concerning the suitability of the three data integrity models for a military environment. As stated in Chapter I, the TCSEC does not contain a standard for enforcement of data integrity. This void needs to be filled, with the three data integrity models presented in this thesis being candidates to fill that void. The goal of the framework developed in Chapter V is to provide a method for producing results that will lead to the recommendation of one model as the most appropriate.

The application in Chapter VI of the framework points out the potential benefits and drawbacks associated with each model. The conclusions reached after analyzing each model within the guidelines of the framework are given below:

(1) While the IWG definition [illegible] integrity is accepted as a standard for application within the framework, there is no agreement in either military or commercial environments as to one acceptable definition to serve as a standard. The primary reason for this is the lack of research in the area of data integrity [Ref. 12]. Because there exist situations in which

unauthorized manipulation may be more harmful than unauthorized disclosure, data integrity is very much a concern in today's computer-based information systems.

(2) There are distinct differences between commercial and military computer environments. The commercial environment is primarily concerned with preventing manipulation of data, thereby preserving data integrity, whereas the military environment has traditionally been concerned with disclosure control. These differences are best pointed out by the Clark\Wilson model, which is based on concepts that are compatible with both environments.

(3) There needs to be increased emphasis in the area of developing the characteristics associated with the term data integrity strictly within the military environment. While it may not be possible to adopt one standard definition, there need to be qualities identified that can be universally applied to all military applications. This is similar to the idea that certain data is considered Top Secret for disclosure purposes regardless of the context in which it is used. Data that is used in a missile launching system can be classified as Top Secret while different data used in nuclear propulsion can likewise be classified as Top Secret. The idea is that there is

a universal classification of Top Secret, regardless of the situation. This idea should be extended to data integrity as well.

(4) The Clark\Wilson data integrity model is the most appropriate model for incorporation into the TCSEC as an integrity standard. The Clark\Wilson data integrity model is recommended for the following reasons:

a. Clark\Wilson has the most appropriate definition for integrity. The integrity definition used in this model is both adequate and complete in respect to the IWG standard. It is sufficiently broad for application in many different environments, including the military environment. Compared to the Biba and Goguen and Meseguer integrity definitions, the Clark\Wilson definition is applicable to a wider range of environments, to include the military environment.

b. Clark\Wilson has a strong relation to secrecy. The ability of the model to limit which data a user can access serves to perform the function of disclosure control. The separation of duties and well-formed transaction concepts limit the ability of any one user to perform all steps in a process. This has the effect of preserving the integrity of the data that is involved in the process.

c. Clark\Wilson identifies the features of a system in which integrity is the primary goal. The model presents nine rules to implement in order to safeguard the integrity of data used in the system. These rules serve as a blueprint for building an effective integrity enforcement system.

d. Clark\Wilson has the potential for integrity labelling similar to military information classification labelling. Presently, this model does not have the capability to attach integrity labels. However, due to its ability to limit the data that each user can access through the separation of duties and well-formed transaction concepts, the addition of this capability is possible. The concepts on which the model is based lend themselves to the addition of an integrity label attachment capability.

It is noted that the Biba model is actually more suitable than Clark\Wilson in this specific area. While Clark\Wilson has potential for integrity labelling, Biba has a greater potential for the successful implementation of labelling. This is due to the relationship of the Biba model to the Bell-LaPadula model for security.

e. Clark\Wilson has no major limitations that cannot be overcome. There are no areas of the model that are deficient enough to overshadow its advantages. The limitations of the model, as described in Chapters IV and VI, are not severe enough to prohibit acceptance.

These conclusions are based on the ideas presented in the appropriate chapters. The framework application in Chapter VI provides the results which can be used to actually select one data integrity model for implementation within military computer environments.

B. RECOMMENDATIONS

Based on the conclusions stated in the above section, the following recommendations are made:

(1) DoD should adopt an integrity model as a part of its security policy. This integrity model should be incorporated into the TCSEC to provide for a complete security policy covering both disclosure control and modification control.

(2) The Clark\Wilson data integrity model should be accepted as the basis for an integrity policy to be incorporated into the TCSEC.

(3) The Clark\Wilson model should be expanded to include the ability to attach integrity labels similar to the security classification labels currently in use for controlled military information.

(4) The TCSEC should adopt a data integrity labelling scheme similar to the scheme which is currently in use for data security. There should be separate levels of integrity classifications with all applicable data identified as to its proper classification. These integrity classifications should restrict both manipulation and modification with mechanisms in place to allow only authorized individuals such privileges. While the integrity labels do not need to be exactly the same as the Top Secret, Secret, and Confidential used for security purposes they do need to have a similar pattern. Labels such as High, Medium, and Low are acceptable provided that the mechanism that enforces integrity is capable of determining authorized access requests from unauthorized requests. There should be three data integrity levels to correspond to the three data security levels.

LIST OF REFERENCES

1. **Department of Defense Trusted Computer System Evaluation Criteria**, Department of Defense Computer Security Center, August, 1983.

2. Biba, K.J., **Integrity Considerations for Secure Computer Systems**, Mitre Corporation, April, 1977.

3. Clark, D.D. and Wilson, D.R., "A Comparison of Commercial and Military Security Policies", **Proceedings of the 1987 IEEE Symposium on Security and Privacy**, April, 1987.

4. Henning, R.R. and Walker, S.A., "Data Integrity vs Data Security: A Workable Compromise", **Proceedings of the 10th National Computer Security Conference**, October, 1987.

5. Goguen, J.A. and Meseguer, J., "Unwinding and Inference Control", **Proceedings of the 1984 IEEE Symposium on Security and Privacy**, April, 1984.

6. Schell, R.R. and Denning, D.E., "Integrity in Trusted Database Systems", **Proceedings of the 9th National Computer Security Conference**, Sept., 1986.

7. Goguen, J.A. and Meseguer, J., "Security Policies and Security Models", **Proceedings of the 1982 IEEE Symposium on Security and Privacy**, April, 1982.

8. Ruthberg, Z.G. and Polk, W.T., **Report of the Invitational Workshop on Data Integrity**, Government Printing Office, 1989.

9. Badger, L., "A Model for Specifying Multi-Granularity Integrity Policies", **Proceedings of the 1989 IEEE Symposium on Security and Privacy**, April, 1989.

10. Schell, R.R., "Evaluating Security Properties of Computer Systems", **Proceedings of the 1983 IEEE Symposium on Security and Privacy**, April, 1983.

11. Chalmers, L.S., "An Analysis of the Differences Between the Computer Security Practices in the Military and Private Sectors", **Proceedings of the 1986 IEEE Symposium on Security and Privacy**, April, 1986.

12. Welke, S., Roskos J., Boone J., and Mayfield T., "A Taxonomy of Integrity Models, Implementations and Mechanisms", **Proceedings of the 13th National Computer Security Conference**, Oct., 1990.

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center 2
Cameron Station
Alexandria, Virginia 22304-6145

2. Library, Code 52 2
Naval Postgraduate School
Monterey, California 93943-5002

3. Commandant of the Marine Corps 1
Code TE 06
Headquarters, U.S. Marine Corps
Washington, D.C. 20380-0001

4. Professor Moshe Zviran, Code AS/Zv 1
Department of Administrative Sciences
Naval Postgraduate School
Monterey, California 93943-5000

5. LTC Rayford B. Vaughn 1
Department of Computer Science
Chauvenet Hall
United States Naval Academy
Annapolis, Maryland 21402

6. CAPT Thomas R. Ivan 2
PLRS System Analyst
PM ADDS, CECOM
Ft. Monmouth, New Jersey 07703-5216

7. Computer Technology Curricular Office 1
Code 37
Naval Postgraduate School
Monterey, California 93943-5000